(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 102 157 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
23.05.2001 Bulletin 2001/21

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **99850176.1**

(22) Date of filing: **22.11.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON**
126 25 Stockholm (SE)

(72) Inventors:
- **Kriens, Peter**
  439 33 Onsala (SE)
- **Danne, Anders**
  164 41 Kista (SE)

(74) Representative: **Sandström, Staffan Sven et al**
Bergenstrahle & Lindvall AB,
P.O. Box 17704
118 93 Stockholm (SE)

(54) Method and arrangement for secure login in a telecommunications system

(57) The invention comprises a method for secure login in a communication system including a mobile unit, a mobile communication network, an authentication center, an application server, a computer and an untrusted network, wherein the user sets up an application session via a data communication from his personal computer to an application server and submitting an identity. Thereat, the server requests authentication from an authentication center. Then, the authentication center sends a simple token to the server, which sends said token to the user over the data connection. Finally, the user reads the token on the screen of his personal computer and sends the token as a text message from the mobile unit to the authentication center, which also obtains the mobile phone number and the cell identification of the user. An advantage of the disclosed method is that no extra pin-code is required.

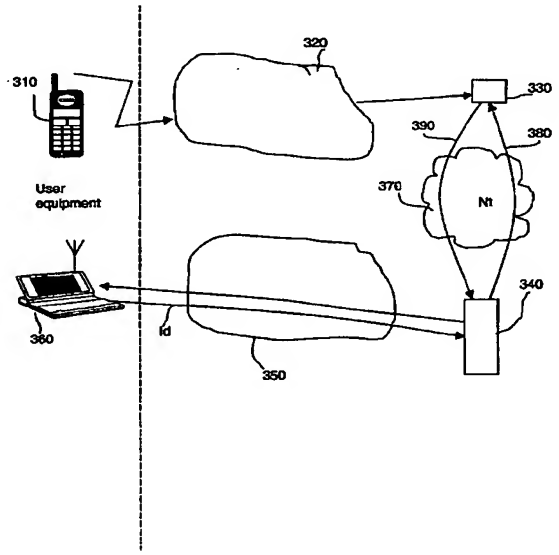


Fig. 3

EP 1 102 157 A1

Description

FIELD OF INVENTION

[0001] The present invention relates to a method and arrangement for secure login over a public network.

DESCRIPTION OF RELATED ART

[0002] In the field of data- and telecommunication, security and particularly methods and arrangements for secure login are demanded. The requirements on security products are increasing.

[0003] In the past, before remote access, organizations had closed, hard-wired networks, which provided physical security. Network access was limited to users physically located in the building. Requiring users to type in a name and password added another layer of security to the network.

[0004] Providing remote network access over telephone lines has added an entirely new dimension to the task of keeping business-critical information secure.

[0005] Conventional telephone systems are, by nature, public. Anyone can dial a number, and reach the "door" leading into a company's network. The primary concern of remote access security is to make sure that only known, authorized users can enter that door.

[0006] While technological advances have redefined the traditional workplace, they have also created more opportunities for security breakdowns. These developments, such as the growth of the Internet and more powerful desktop systems, are placing a greater burden on those responsible for the security of an organization's computing resources. For example, the explosion of the Internet has compounded security issues by combining public and private network access, resulting in a new category of security requirements that must be addressed.

[0007] Security considerations have been further complicated by the multiplicity of functions and applications that are now accessible at the PC. Because every application handles security in a different way, most users cannot access all of their applications through a single password. The need to remember multiple passwords can lead to a natural temptation to repeat or simplify passwords. Consequently, multiple levels of security can have the unintended effect of actually compromising security.

[0008] Larger organizations having global multi-point access requirements, and those having greater security concerns, wants to integrate their remote access capabilities with products specifically designed to enhance the security of information distributed over remote networks.

[0009] One alternative approach is "centralized" security, which involves having the terminal or communications server authenticate a dial-in user's identity through a single central database, known as the authentication server. This server stores all the necessary information about users, including their password and access privileges. The use of central location for authentication data allows a greater degree of security for sensitive information, greater ease of management and a more scalable solution as the size of the network increases. Authentication servers can be configured in a variety of ways, depending upon the organization's preferred network security scheme.

[0010] Authenticating a user includes the following steps:

- A user dials into a network through a remote access server.
- The remote access server forwards the user identification and password to the authentication server.
- The authentication server validates and provides access privileges to the user.

[0011] Many of the most popular remote access security enhancements operate on the principle of "security by secrecy", wherein users must have a specific object in their possession to access the network. The "secrecy" of that object creates a much larger hurdle for attackers. Security by secrecy refers to people using a complicated mechanism that is hard to know. E.g. an unlisted telephone line, but it is assumed that the number of said phone line is unknown to the public. A password is security by secrecy. The owner of the password must be the only one that should know this password.

[0012] One of the most popular methods for promoting security by obscurity is through a "smart card", which is simply a credit card containing a small, built-in computer. Not anyone who comes into possession of a smart card can use it, unless he has access to another piece of confidential information - the user password. Smart cards also help solve the problem of having to remember multiple passwords, as disclosed above.

[0013] The concept of a one-time password involves having the security server already know that a password is not going to be transmitted over insecure channels. When the user connects, he or she receives a challenge from the security server. The user takes the challenge information and uses it to calculate the response from the password. Thereat, the security server calculates the response, and compares its answer to that received from the user. The password is never transmitted over the network; nor is the same challenge used twice (e.g. RACOM, Remote Access COMmunication).

[0014] Some of these products, such as secureID, use a time-based temporary password system. When users dial in to the server, they are prompted to enter a personal identification number (PIN), along with the six-digit number currently showing on their hand-held card and password. This number changes every minute at

the same time as a corresponding number on the server, making it virtually impossible to gain access to the network without the card.

[0015] The telecommunication operator Tele2 has recently developed a system called GiSMo for a mobile telecommunication system in order to authenticate a user, when he wants to make a purchase. The GiSMo system uses a GSM (Global System for Mobile communication) telephone and corresponding GSM number as a unique identity. The telephone is opened by means of the ordinary Pin-code of the owner of the telephone and a 070-number being a personal number of the owner. At each GiSMo transaction, the user is provided with a unique code by means of a text message, e.g. a Short Message Service (SMS), to the activated GSM telephone. Said unique code can only be used for the ongoing transaction. The code is verified when the owner input it on the PC. A disadvantage with the GiSMo system provided by telecom operator Tele2 is that the text message may be eavesdropped.

SUMMARY OF THE INVENTION

[0016] A problem with the above disclosed methods using a smart card, such as a SIM (Subscriber Identity Module) card, is that it may take some time before the loss of such a smart card is disclosed and the usage of said card is blocked.

[0017] A problem with the methods according to prior art is that an extra code must be provided and used.

[0018] A further problem with methods according to prior art is that an extra device is required.

[0019] The invention comprises a method and arrangement for secure login in a communication system including a mobile unit, a mobile communication network, an authorization center, an application server, a computer and an untrusted network, wherein the user sets up an application session via a data connection from a personal computer to an application server and submits an identity to the authentication center. Thereafter, the application server requests authentication of this session from an authentication center. Then, the authentication center answers with a simple token to the application server, which sends said token to the user over the data connection. Thereupon, the user reads the token on a screen of the personal computer and sends the token as a text message, e.g. a Short Message Service (SMS), from the mobile unit to the authentication center. This authentication request message is generated from an application running inside the mobile unit and contains the token as entered by the user appended with the global unique identity of the cell where the message was sent from as available inside the mobile unit. The mobile unit will then send this message though the mobile communication network. Systems inside the mobile communication network extend the message with current time and A-number of the sending mobile unit and forward this extended message to the authentication center. Finally, the message arrives within a certain time in the authentication center where the token is used to match it to the application session. There the A-number and the cell identity are verified against the given identity for that session. Both A-number and cell identity must be allowed for the given user identity. If optionally other authentication mechanisms like for example time are satisfied, the authentication center sends a message to the application server informing the application server that the user is correctly authenticated. When no message arrives within a certain time or a message with an A-number not associated with the user identity or a message with a cell identity not associated with the user identity then the Authentication Centers sends a message to the application server that the session is not authenticated. If a message arrives after a certain time, it is discarded.

[0020] The method as disclosed herein may be implemented by means of a computer program.

[0021] The main purpose of the method as disclosed herein is to provide a secure method for secure login, wherein a mobile access unit, such as a mobile telephone, is used instead of a smart card.

[0022] A purpose of the method disclosed herein is to provide a secure method and arrangement for remote login.

[0023] An advantage of the method as disclosed herein is that no extra pin-code is required.

[0024] A further advantage of the method as disclosed herein is that no extra device is required.

[0025] A yet further advantage of the method as disclosed herein is that the loss of the phone is discovered earlier than the loss of a smart card, and actions to address said loss may be taken sooner.

[0026] The term "comprises/comprising" when used in this specification is taken to specify the presence of stated features, integers, steps or components but does not preclude the presence or addition of one or more other features, integers, steps, components or groups thereof.

[0027] Further scope of applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0028]

Figure 1 is a sequence diagram illustrating a method according to prior art.

Figure 2 is a sequence diagram according to the invention

Figure 3 is an overview of the system according to the invention.

[0029] The invention will now be described in more detail with reference to preferred exemplifying embodiments thereof and with reference to the accompanying drawings.

DETAILED DESCRIPTION

[0030] The method according to the invention will now be disclosed with reference to fig. 2 and 3. In the method disclosed herein a cellular telephone 310 provided with a PIN number is used instead of a special key card device. A text service, such as Short Message Service (SMS), is used for communication at login.

[0031] In a system implementing the method disclosed herein and illustrated in fig. 2, a personal computer (PC) 360 is connected to a application server 340 over an untrusted network such as the Internet. The personal computer 360 has only access to the application server when it is used by an authorized person (not shown in the figure).

[0032] In a first step, the user sets up a data communication from his personal computer 360 to an application server 340, via a network 350, and provides an identity Id. Thereafter, in a second step, the application server 340 contacts an authentication center 330 over a trusted network Nt 370 with a request 380 to authorize the given identity Id. In a third step, said authentication center 330 responds 390 with a unique challenge token, which is sent over the same data connection in the trusted network Nt 370. The token is not secret and may be predictable. The token is valid for a limited time. Thereat, in a fourth step, the user reads the token on the screen of his computer 360 and sends it back as a text message via the cellular telephone 310 to the authentication center 330 that also receives the phone number and the current cell identity associated with the cellular phone 310. The cell identity indicates the geographical location of the cellular phone 310. Depending on how the mobile communication system is designed, a mobile unit, such as the cellular telephone 310, may have one or more cell identities. In a fifth step, the authentication center checks that the text message arrives within a certain time provided with the correct token from one of the valid geographical positions. The authentication center 330 is provided with a table for each user, wherein each record comprises the identity, cellular telephone number, and valid cell identification of the user.

[0033] The token used in the method as disclosed must fulfill certain requirements. The token must be keyed in by the user. The token may consist of e.g. a 4-integers key. In an exemplary embodiment, a method using "voice recognition" may be used.

[0034] In order to implement the method as disclosed in this disclosure, a computer (not shown in the drawings) may be located in, or connected to, the authentication center 300. Said computer may be loaded with software portions for performing the method disclosed in this disclosure. In a further embodiment, said method may be implemented as hardware in a computer.

[0035] In a further embodiment, after that the application server has requested authentication to the authentication center, the authentication center sends a text message, e.g. a Short Message Service (SMS), to the telephone that needs to be replied to. Thereafter, the user replies with a positive confirmation, e.g. "Y". This procedure is more costly, but has the advantage that the application server does not require a special login UI (User Identity). E.g. in an exemplary application server, no UI is involved, and adding a login screen would be awkward. When a user of said application server uses a network address inside an intranet, an text message is sent. If said text message is acknowledged, access is allowed, otherwise, access is denied.

[0036] In a further embodiment of the invention a combined terminal, such as a smart telephone or a WAP (Wireless Application Protocol) telephone may be used instead of a mobile phone and a computer.

[0037] In a yet further embodiment, the phone sends automatically the token back as a text message.

[0038] A faked text message may only be sent from inside an operator, by means of spoofing an A-number. This can be prevented by putting an extra key in the telephone and signing the message by means of this signature key. However, this is only feasible when the secret key, e.g. the PIN number, is unknown to the operator. In a further embodiment, encryption may be used instead of signing

[0039] The invention being thus described, it will be obvious that the same may be varied in many ways. Such variations are not to be regarded as a departure from the spirit and scope of the invention, and all such modifications as would be obvious to one skilled in the art are intended to be included within the scope of the following claims.

Claims

1. Method for secure login in a communication system including a mobile unit (310), a mobile communication network (320), an authentication center (330), an application server (340), a computer (360) and an untrusted network (350), **characterized** in further comprising the steps of

   - A user setting up a data connection from a personal computer to an application server and submitting an identity to said authentication center (330)

   - The application server (340) requesting authentication from an authentication center (330)

- The authentication center (330) sending a simple token to the application server (340), which sends said token to the user over the data connection

- The user reading the token on a screen of the personal computer and sending the token as a text message from the mobile unit (310) to the authentication center (330), which also obtains a mobile phone number and a cell identification associated with the mobile unit (310).

- Provided that the text message arrives at the authentication center (330) within a certain time along with an acceptable token from one of the valid geographical positions as defined by the cell identification, the authentication center (330) sending an authentication to the application server (340).

2. Method according to claim 1, **characterized** in that the authentication center (330) is provided with a table having a record for each user comprising user identity, mobile phone number and valid cell identification.

3. Method according to claim 1, characterized in that a combined terminal is used instead of a mobile phone and a personal computer.

4. Method according to claim 3, **characterized** in that the combined terminal is a so-called smart phone.

5. Method according to claim 3 **characterized** in that the combined terminal is a Wireless Application Protocol (WAP) telephone.

6. Method according to claim 1, **characterized** in that the token is sent in a text message, from the authentication center (330).

7. Method according claim 6, **characterized** in that said message is a Short Message Service (SMS) message.

8. Method according to claim 1, **characterized** in that the token is automatically returned in a text message.

9. Method according to claim 8, **characterized** in that the text message is an SMS message.

10. A computer program product directly loadable in the internal memory of the authentication Center (330), **characterized** by comprising software portions for performing the method according to any of claims 1-9, when the authentication center is activated by a computer or a signal.

11. An arrangement for secure login in a communication system including a mobile unit (310), a mobile communication network (320), an authentication center (330), an application server (340), a computer (360) and an untrusted network (350), **characterized** in that the arrangement comprises

- Means for enabling a user to set up a data connection from a personal computer to an application server and to submit an identity to said authentication center (330)

- Means for enabling the application server (340) to request authentication from an authentication center (330)

- Means for enabling the authentication center (330) to send a simple token to the application server (340), which sends said token to the user over the data connection

- Means for enabling the user to read the token on a screen of the personal computer and to send the token as a text message from the mobile unit (310) to the authentication center (330), which also obtains a mobile phone number and a cell identification associated with the mobile unit (310),

- Provided that the text message arrives at the authentication center (330) within a certain time along with an acceptable token from one of the valid geographical positions as defined by the cell identification, means for enabling the authentication center (330) to send an authentication to the application server (340).

12. An arrangement according to claim 11, **characterized** in that the authentication center (330) is provided with a table having a record for each user comprising user identity, mobile phone number and valid cell identification.

13. An arrangement according to claim 11, **characterized** in that a combined terminal is used instead of a mobile phone and a personal computer.

14. An arrangement according to claim 13, **characterized** in that the combined terminal is a so-called smart phone.

15. An arrangement according to claim 13, **characterized** in that the combined terminal is a Wireless Application Protocol (WAP) telephone.

16. An arrangement according to claim 11, **characterized** in that the token is sent in text message, from the authentication center (330).

17. An arrangement according to claim 11, **characterized** in that the token is automatically returned in text message.

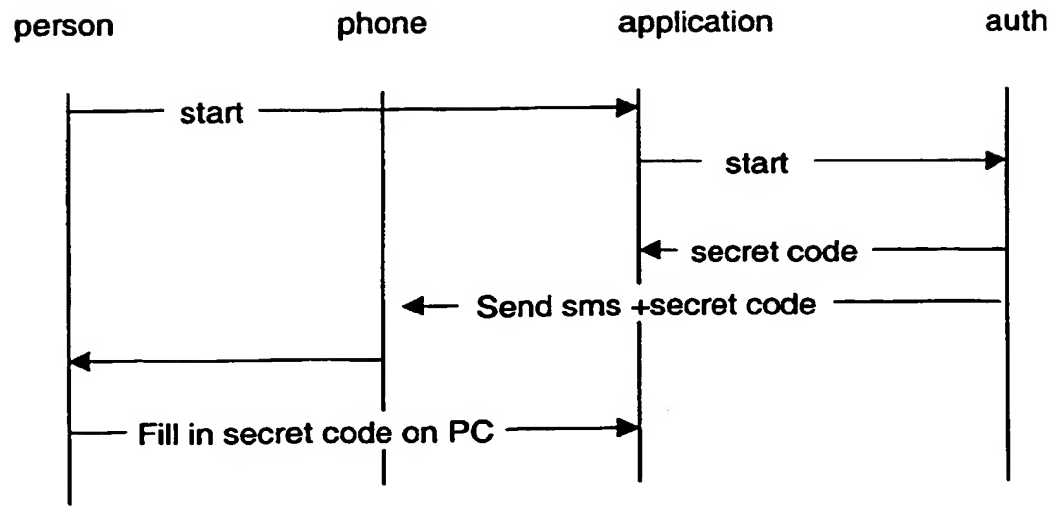


Fig. 1

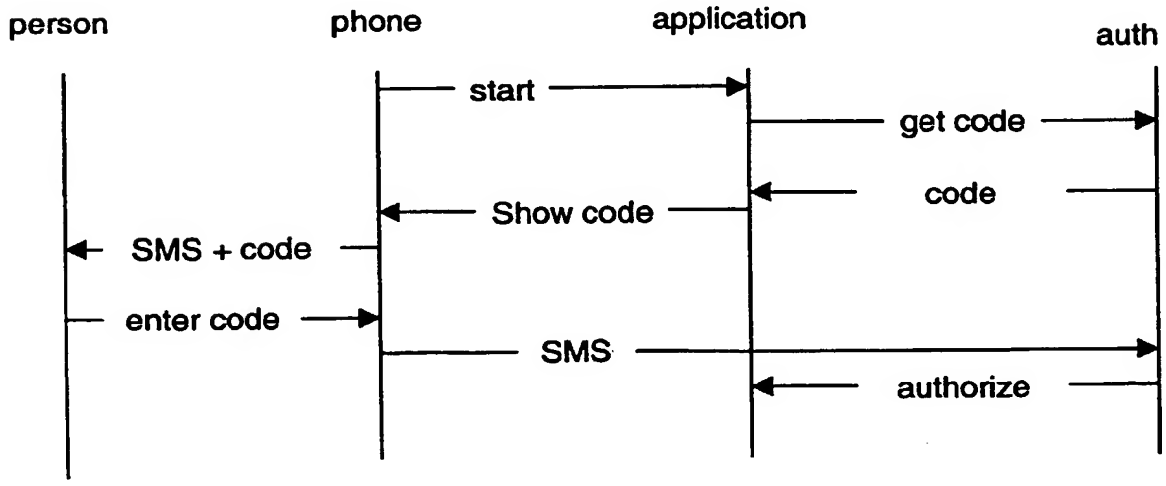
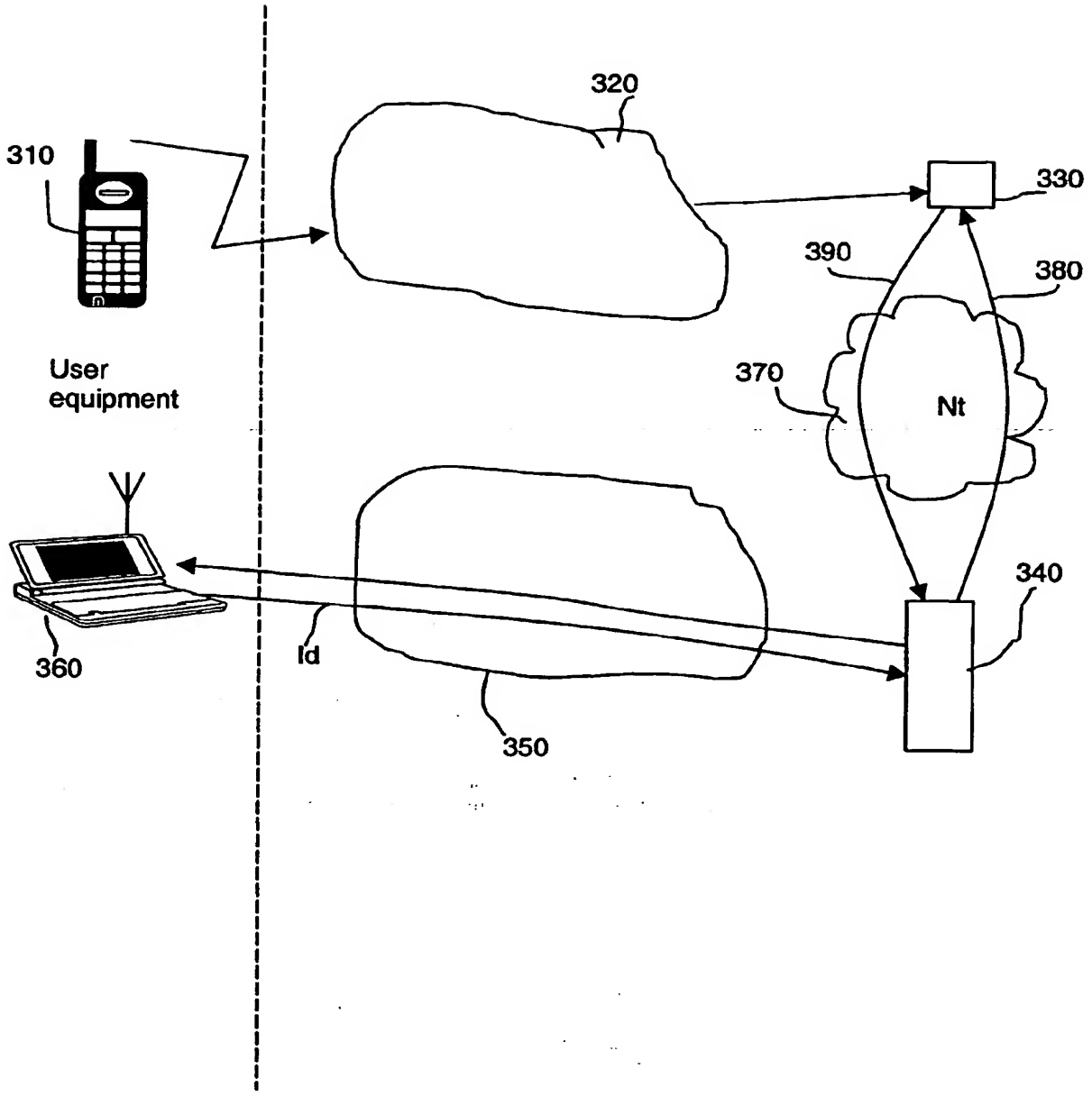


Fig. 2



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 85 0176

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
E	WO 00 03316 A (ERICSSON TELEFON AB L M) 20 January 2000 (2000-01-20) * page 2, line 27 - page 3, line 2 * * page 4, line 5 - line 9 * * page 12, line 9 - page 13, line 19 * * page 14, line 5 - line 8 * * page 15, line 24 - page 16, line 16 *	1,10,11	G06F1/00
A	WO 99 44114 A (ERICSSON TELEFON AB L M) 2 September 1999 (1999-09-02) * page 8, line 6 - line 8 * * page 8, line 18 - line 27 * * page 21, line 18 - line 25 *	3-5, 13-15	
A	WO 97 31306 A (NOKIA MOBILE PHONES LTD ;KURKI TEEMU (FI); SORMUNEN TONI (FI)) 28 August 1997 (1997-08-28) * page 5, line 33 - page 6, line 30 * * page 8, line 24 - line 35 *	1,6,7, 11,12,16	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

H04L
H04Q
G07F
G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
BERLIN	12 April 2000	Rothlübbers, C

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 99 85 0176

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

12-04-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0003316 A	20-01-2000	NONE	
WO 9944114 A	02-09-1999	FI 980427 A	26-08-1999
		AU 2831699 A	15-09-1999
WO 9731306 A	28-08-1997	FI 960820 A	24-08-1997
		AU 1604497 A	10-09-1997
		EP 0976015 A	02-02-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82